MILITARY HEALTH SYSTEM (MHS) **INFORMATION ASSURANCE (IA)** **IMPLEMENTATIONTION GUIDE**	**IMPLEMENTATION GUIDE No. 10**	
	EFFECTIVE DATE 07/19/05	**REVISED DATE** xx/xx/xx

Subject:

SYSTEM LIFE CYCLE MANAGEMENT

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

The term “MHS Information System (IS)” encompasses all automated IS applications, enclaves, outsourced IT-based processes, and platform information technology (IT) interconnections as defined in DoD Instruction (DoDI) 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003.

The MHS Information Assurance (IA) System Life Cycle Management (LCM) process ensures required security safeguards are developed and executed to protect ISs against accidental or intentional unauthorized modification, disclosure, destruction, and denial of service throughout the life cycle of the system. Including security early in the IS development life cycle, rather than adding it to an operational system, will usually result in less expensive and more effective security.

This implementation guide provides direction on the scope of IA elements to be considered during the system development life cycle and when integrating IA into the acquisition process. IA shall be considered in all phases of the LCM process and shall be included in the preliminary acquisition implementation strategy. Identifying IA safeguards early in the acquisition implementation strategy will ensure that key elements, such as technical security requirements, scheduling, and cost and funding issues associated with executing requirements for IA are addressed and maintained. IA requirements shall be incorporated in the early stages of program design activities to ensure the appropriate confidentiality, integrity, availability, authenticity, and non-repudiation of the system information are protected in accordance with references (a) through (l) in section 4. As part of the incorporation of IA in the early stages, the Certification and Accreditation (C&A) staff should be included in the process to ensure C&A can be completed smoothly. IA is considered an integral segment of security LCM and the acquisition process.

2 POLICY

It is MHS Policy that:

2.1 IA requirements be identified and included in the design, acquisition, installation, operation, and upgrade or replacement of MHS ISs.

2.2 Required IA Controls are implemented to protect MHS ISs against unauthorized modification, disclosure, destruction, and denial of service throughout the security development life cycle phases.

2.3 As early as possible in the life cycle of IT-dependent programs, information owners shall establish the mission assurance category (MAC), security classification, sensitivity, and need-to-know of information and information systems.

2.4 The IA controls are established as part of the baseline requirements consistent with DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and are implemented throughout the system's life cycle. DoDI 8500.2 provides a detailed list of the IA controls necessary to achieve the baseline levels of confidentiality, integrity, and availability.

2.5 TMA Components shall, at a minimum:

a. Develop security specifications based on DoD IA Controls.

b. Identify risk areas and define risk reduction measures, management approaches, and plans.

c. Test and evaluate to certify that technical security features and other safeguards satisfy specified security requirements before the initiation of operational testing.

d. Establish procedures to ensure continuous use of approved security safeguards during the production, deployment, implementation, and operational/maintenance phases.

e. Ensure IA requirements are addressed and incorporated into the acquisition documentation in accordance with DoDI 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004.

3 PROCEDURES

3.1 IA LCM incorporates operational requirements for security in all IS planning and design, and ensures conformance with applicable security regulations, policies, and requirements. The product of this activity is the Information Assurance Strategy. The TMA Component sponsoring the system development shall have an understanding of the nature, need, and information processed by the system to determine the information's sensitivity and criticality.

3.1.1 Security System Life Cycle Management Phases

Security planning shall be implemented throughout a system life cycle. At a minimum, the TMA Component shall incorporate the following security into the system life cycle:

a. Initiation Phase

- Security Categorization – defines the MAC level to establish the IA controls based on confidentiality levels. Designation of a MAC level assists the TMA Component in identifying the appropriate security controls based on the sensitivity of the information.
- Preliminary Risk Assessment – results in the initial description of the basic security needs of the system. A preliminary risk assessment defines the threat environment in which the system will operate.

b. Acquisition/Development Phase

- Risk Assessment – analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation Phase, but is more in-depth and specific.
- Security Functional Requirements Analysis – analysis of requirements that may include the following components: (1) system security environment (policies and architecture) and (2) security functional requirements.
- IA Controls Analysis – analysis of IA controls that address the required development activities and the assurance evidence needed to produce the desired level of confidence in the accuracy and effectiveness of the information security. This analysis shall ultimately become part of the baseline IA security requirements.
- Cost Consideration and Reporting – determines the amount of development attributed to information security over the life cycle of the system. This cost includes hardware, software, personnel, and training.
- System Security Authorization Agreement Planning – ensures that IA controls are planned, agreed upon, in place, and fully documented. The security plan shall also provide a complete characterization or description of the IS, as well as the attachment of references to key documents and programs supporting the IS security program (e.g., configuration management plan, contingency plan, incident response plan, Information Assurance Vulnerability Management (IAVM), security awareness and training, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, certification and accreditation, and plan of action and milestones).
- IA Control Development – ensures that IA controls are described in the security plans and are implemented consistent with the DoD. For ISs currently in operation (e.g., legacy systems), the security plans may call for additional IA controls or modification of existing IA controls.
- Developmental Security Test and Evaluation – ensures that IA controls chosen and developed for a new IS are working properly and effectively.

- Other Planning Components – ensures that all components of the development process are considered when incorporating IA into the life cycle. These selections include appropriate contract type, participation by all related functional groups, participation by certifier and accreditor, and development and execution of necessary contracting plans and process.

c. Implementation Phase

- Inspection and Acceptance – ensures that the MHS IA Program Office and local Designated Approving Authority (DAA) validate and verify that the functionality described in the specification is included in the deliverables.
- Security Control Integration – ensures that IA controls are integrated at the operational site where the IS is to be deployed for operation. Security control settings and switches are enabled in accordance with DoD directives.
- IA Certification – ensures that the IA controls and MAC designation are effectively implemented through the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and appropriate safeguard measures are in place.
- IA Accreditation – ensures the appropriate DITSCAP accreditation is granted by the authorized Certification Authority and DAA based on the effectiveness of IA controls in place.

d. Operation/Maintenance

- Configuration Management and Control – ensures adequate consideration of the potential security impacts due to specific changes to an IS or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the IS, subsequently controlling and maintaining an accurate inventory of any changes of the system.
- Continuous Monitoring and Testing – ensures that controls continue to be effective in their application through periodic, unannounced, in-depth monitoring and testing to be reported to the MHS IA Program Office. This includes specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD Information Assurance Vulnerability Alert (IAVA) or other DoD IA practices that are planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

e. Disposition Phase

- Information Preservation – ensures that information is retained, as necessary, to conform to the DoD sensitive information protection requirements.
- Media Sanitization – ensures that hardware and software are disposed of in accordance with current DoD policy and the applicable MHS IA policy implementation guide.

3.1.2 Acquisition Program Manager (PM) Responsibilities

At a minimum, the PMs for acquisition programs shall:

a. Remain ultimately responsible for the platform's overall IA protection for acquisitions of platforms with internal information technology (IT), including platforms such as medical technologies or utility distribution systems.

b. Retain responsibility to incorporate all IA protective measures necessary to support the platform's support mission functions for acquisitions of platforms with IT that do not interconnect with external networks.

c. Identify all assurance measures needed to ensure both the protection of the network and the protection of the platform from connection risks, such as unauthorized access, that may be introduced from the network.

d. Demonstrate prudent judgment by considering the IA program provisions in DoD Directive (DoDD) 8500.1 and DoDI 8500.2 for systems that are not connected to external networks and that do not involve internal networks, and employing those IA controls appropriate to their system.

e. Be responsible for coordinating with enclaves that host (run) Automated Information Systems (AISs) applications early in the acquisition process to address operational security risks the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement.

f. Comply with the IA requirements in the DoD 8500 policy series for acquisitions of outsourced IT-based processes.

g. Be responsible for employing the sets of baseline controls appropriate to their programs.

4 REFERENCES

a. ASD (C3I) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001

b. Assistant Secretary of Defense (Health Affairs) Memorandum, "Military Health System Information Assurance Policy Guidance," March 5, 2004

c. DoDD 5000.1, "The Defense Acquisition System," May 12, 2003

d. DoDI 5000.2, "Operation of the Defense Acquisition System," May 12, 2003

e. DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002

f. DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

g. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002

h. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

i. DoDI 8580.1, “Information Assurance (IA) in the Defense Acquisition System,” July 9, 2004

j. Federal Information Security Management Act of 2002

k. NIST Special Publication 800-64, “Security Consideration in the Information System Development Life Cycle,” October 2003 (Revised July 7, 2004)

l. Health Insurance Portability and Accountability Act (HIPAA) Security Final Rule, February 20, 2003.

5 ACRONYMS

AIS	Automated Information System
DAA	Designated Approving Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
IA	Information Assurance
IAM	Information Assurance Manager
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IS	Information System
IT	Information Technology
JMISO	Joint Medical Information Systems Office
LCM	Life Cycle Management
MAC	Mission Assurance Category
MHS	Military Health System
PEO	Program Executive Office
PM	Program Manager
TMA	TRICARE Management Activity
TRO	TRICARE Regional Office